Principal Computer Security Officer
(Information Systems Specialist)

DESCRIPTION
The Principal Computer Security Officer is a position located within the Information Security Services unit in ITSS, which itself includes (1) responsibility for information security strategy, security architecture development, and information system security practices; (2) both proactive and operational responsibility for incident intrusion prevention/detection, investigation, and response; and (3) organized programs of information security consulting and outreach. The scope of this unit covers all utilized enterprise technologies, including mainframe, distributed, infrastructure-based, personal, and desktop systems at Stanford University.

The Principal Computer Security Officer reports to the Director of Information Security Services and is the senior technical information security leader/specialist in the unit. The primary goal of the person in this role is to help Stanford ensure an appropriate level of security over information processing resources while preserving and enhancing system usability. This person will provide technical leadership to other members of the group and advice and counsel to the Director of ISS on both technical and strategic information security matters.

Responsibilities include:

- Serve as the senior information security leader/specialist for developing proactive approaches to improving Stanford’s general information security posture. May be asked to provide management and/or supervisory support to any of Information Security Services’ organizational units.
- Provide technical leadership, expertise, and education working with technical staff for the inclusion of network security throughout the design, development, and deployment of academic and administrative information systems. Perform security assessments with and for both information system projects and information systems in production sometimes in conjunction with Internal Audit.
- Provide expertise for system administrators and technical staff to ensure conformance to security policy standards. Assist schools, departments, and administrative offices in applying best practices in securing the data and information systems under their control.
- Participate in the development and documentation of information security standards, best practices, and guidelines. Assist the Director of Information Security Services in the development of information security strategy, architecture, and policies.
- Maintain a state-of-the-art awareness of information security issues, incident types and directions, problems, utilities, and solutions for all major information system platforms typically in use at Stanford.
- Bring non-conformance to information security standards to the attention of the Director of Information Security Services.
- Pro-actively monitor the security levels of information systems campus-wide.
- Work with law enforcement agencies when necessary concerning potential criminal matters related to computer and information system security incidents. Work with Stanford-internal regulatory and enforcement offices (e.g., Legal Office, Judicial Affairs Office, Internal Audit Department) on information security and privacy related matters.
- Represent campus security requirements as necessary to vendors of workstations, connectivity equipment, and other information technologies and also to appropriate security agencies.
- Evaluate utilities and tools for enhancing and/or monitoring information security.
- Work with other members of the team on security incident and intrusion handling and resolution.
QUALIFICATIONS/EXPERIENCE
This person must be able to develop and implement flexible security solutions, dictated by the needs of a hybrid and rapidly evolving centralized/decentralized academic and business environment. The individual must be (1) a technically capable person with direct experience in information security; (2) a service-oriented person who is able to gain cooperation from others; and (3) a results-oriented person who can achieve tangible improvements in the data security arena.

The successful candidate will have the following:

- Bachelor's degree in computer science, an equivalent degree, or equivalent experience; a minimum of 10 years computing and information systems experience; and at least 6 years experience in computing and information systems security. Advanced degree and/or course work in information security highly desirable.
- Thorough and demonstrated knowledge of Sun, Linux, IBM, SGI and Microsoft operating systems, general UNIX and Windows system administration practices and skills, understanding of networking principles, practices and technologies (particularly the TCP/IP Internet and related protocols) and networking configuration knowledge.
- Strong understanding of security issues, problems, utilities, techniques, and solutions. Excellent skills in troubleshooting and monitoring also required. Experience in handling security incidents/intrusions.
- Knowledge of authentication protocols (e.g., Kerberos, SSH). Understanding of encryption standards and protocols (e.g., public-key, RSA, PGP, and PEM).
- Customer services experience a requirement. Demonstrated ability to communicate effectively, both verbally and in writing.
- Experience working with academic clients and knowledge of vendor technical support procedures is desirable.
- High level of integrity and excellent judgment concerning privacy issues.
- Demonstrated ability to work as a cooperative team member across all levels and organizations (i.e., ISS, ITSS, and Stanford) in a dynamic environment and to support adherence to policies in an authoritative but non-dictatorial manner.
- Supervisory and/or management experience highly desirable.